California Department of Corrections and Rehabilitation / California Prisons Health Care Services

Directory Services Roadmap
Architectural Considerations

Version 1.04

California Department of Corrections and Rehabilitation / California Prisons Health Care Services: Architectural Considerations
Directory Services Roadmap

Version: 1.04

Date: 14 August 2009

Table of Contents

Table of Contents

California Department of Corrections and Rehabilitation / California Prisons Health Care Services:
Architectural Considerations
Directory Services Roadmap

Version: 1.04

Date: 14 August 2009

Executive Summary

The California Prison Health Care Receivership (CPR) was mandated to improve medical care in the California Department of Corrections and Rehabilitation (CDCR). Once improvements have been made, the receivership will return control of prison health care services to the state. In the context of information technology, sufficient improvements must be achieved in keeping with the asserted mandate.

Until recently, it was planned to move email services for California Prisons Health Care Services (CPHCS) into a separate infrastructure from CDCR. Instead, CDCR and CPHCS will continue to cohabitate on the same email system and transition to the shared services email infrastructure provided by the California Department of Technology Services (DTS). In the absence of the requirement for a separate email system in the CPHCS data center, contributing factors for the directory services architecture should be assessed. This document provides considerations for the directory services roadmap for California Department of Corrections and Rehabilitation (CDCR) and California Prisons Health Care Services (CPHCS).

1.   Introduction

As a result of the recent decision to use a single Exchange organizational structure for CDCR and CPHCS, a meeting on March 26, 2009 to assess the technology roadmap with respect to directory services was conducted. Participants included technology representatives from EIS, CPHCS, D&T/CDR, ENS, Microsoft, and EMC/Janalent and additional review was provided by Angus-Hammer. See section "7 Attendees and reviewers" on page 11 for a list of attendees and reviewers.

1.1   Purpose

This document is intended to raise awareness of the impacts of different roadmaps by assessing options for directory services architectures based on input from directory services stakeholders and subject matter experts at CDCR and CPHCS.

1.2   Scope and layout

This document provides principles and corresponding business requirements of CDCR and CPHCS (based on attendees' understanding). Subsequently, options for directory services architectures are assessed for their ability to meet needs of CDCR and CPHCS.

2.   Principles

In the context of this document, principles are intended to capture the shared vision of the CDCR and CPHCS so that all design decisions can be measured by a common understanding of success. In general, the technology roadmap for CDCR and CPHCS are guided by the following principles:

- Meet the mandate of the receivership to improve healthcare services in the California prisons, which includes achieving a HIPAA-compliant environment.
- Comply with state guidelines to centralize email services at DTS.
- Minimize cost, complexity and impact on end-users and administrators; maximize flexibility and scalability.

3.   Business requirements

Based on the input and understanding provided by meeting attendees, the following business requirements have been recorded:
- HIPAA compliance
    - Auditing
    - Role-based access control (RBAC)
    - Encryption
        - Volume

California Department of Corrections and Rehabilitation / California Prisons Health Care Services:
Architectural Considerations
Directory Services Roadmap

Version: 1.04

Date: 14 August 2009

- - - Transaction
  - o Network access (802.1x)
- Migration process
  - o Full coexistence
- Directory services
  - o CPHCS application deployment
    - Dictation and Transcription (D&T) – Thick-client
    - Clinical Data Repository (CDR) – Web-based portal
  - o Schema changes
- The following applications must be supported:
  - o Fax
  - o Unified messaging
  - o Office Communication Server (OCS)
  - o RMS (email, file, SharePoint)
  - o Prolaw
- Messaging and collaboration services
  - o CDCR and CPHCS should continue to collaborate and coexist

4.   Current directory services architecture

At present, the current directory and messaging architecture is summarized in Figure 1, below.
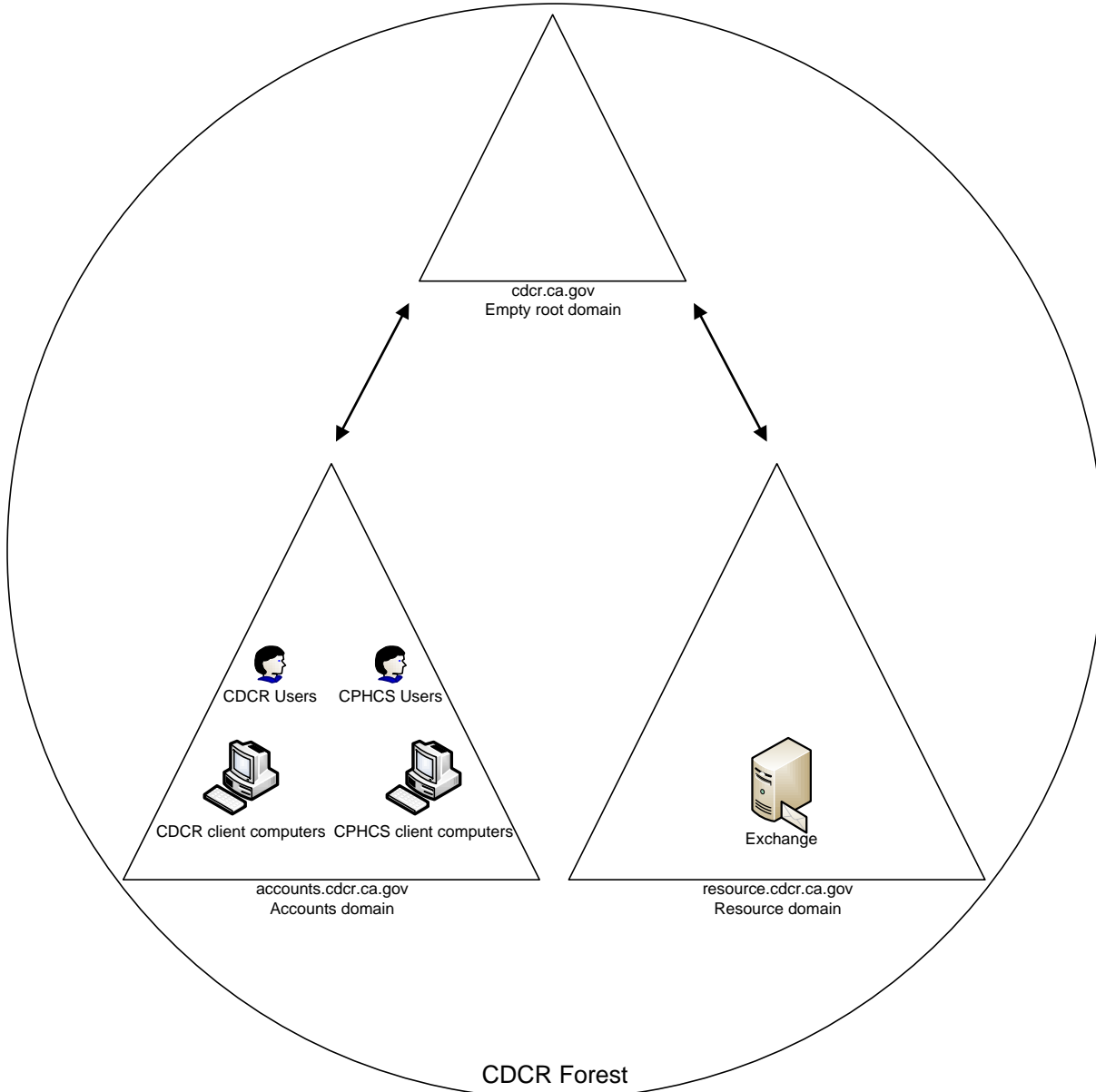

Figure 1 Current directory services architecture
In the current architecture, CDCR and CPHCS accounts and Exchange resources are located in a single forest.

California Department of Corrections and Rehabilitation / California Prisons Health Care Services: Architectural Considerations
Directory Services Roadmap

Version: 1.04

Date: 14 August 2009

5. Future directory services architecture

There are two options considered in this document:

- Scenario 1 consists of one forest for CDCR users, one forest for CPHCS accounts and applications, and one forest for Exchange resources at DTS (see Figure 2, below)
- Scenario 2 consists of one forest for both CDCR and CPHCS accounts, one forest for CPHCS applications, and one forest for Exchange resources at DTS (see Figure 3, below)
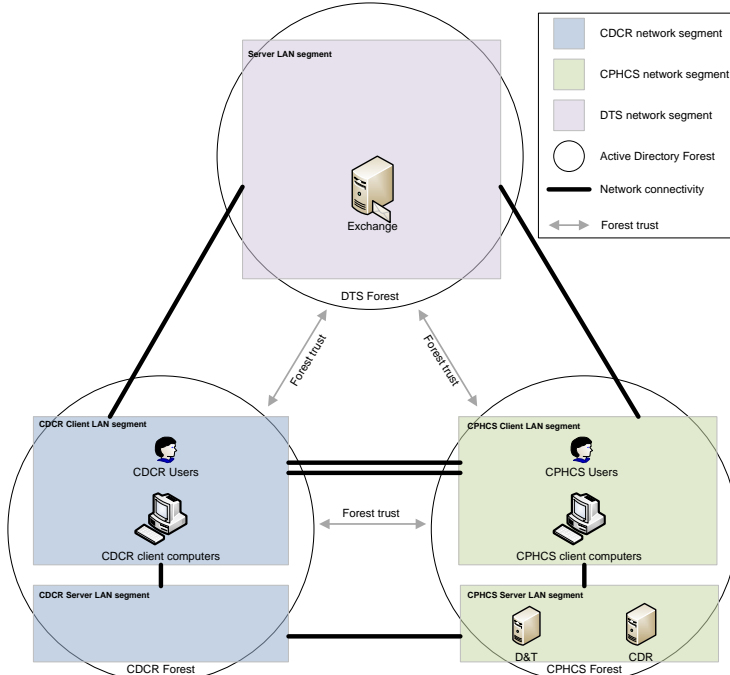

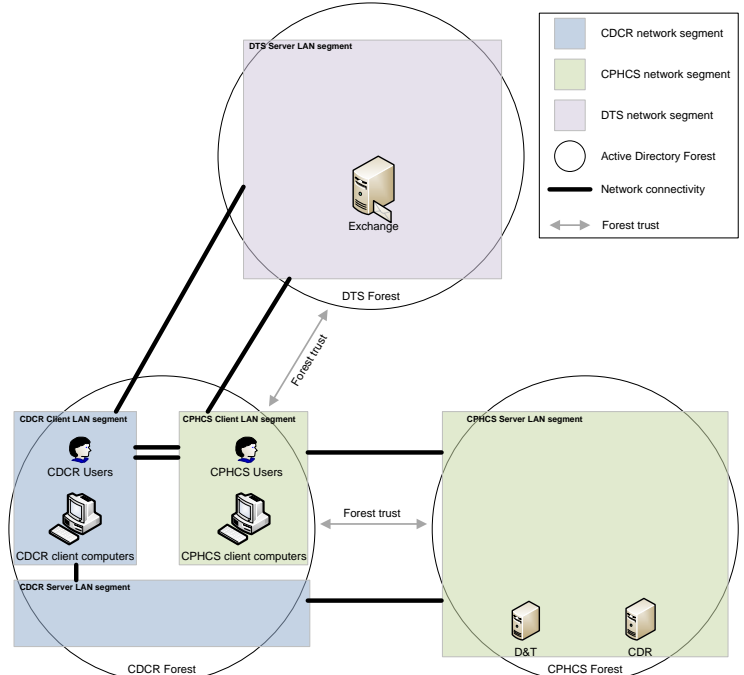**Figure 2: Scenario 1 directory/messaging roadmap**

Figure 3: Scenario 2 directory/messaging roadmap

Both scenarios share the following characteristics:

- A plan for HIPAA compliance will be established.
- The CPHCS forest will host health care applications
  - o Note: Migration of users and computers to the CPHCS forest is <u>NOT</u> required to access applications securely or to achieve role-based access controls.
- Verizon will manage the CPHCS forest and applications.
- Verizon IT will provide support for CPHCS and have delegated authority over their users and computers.
- Email will be migrated to DTS.
- A forest trust will be created between the CDCR forest and the CPHCS forest.
- Objects and assets will be delineated between CDCR and CPHCS.
- CPHCS computers will be physically re-cabled to the new CPHCS network segments.
- Performance of LAN-to-LAN connectivity at each institution will be required.

Differences:

- CPHCS user and computer objects would be migrated to the CPHCS forest in Scenario 1; CPHCS user and computer objects would remain in the CDCR forest in Scenario 2.
- A forest trust between the CPHCS forest and the DTS forest would be required in Scenario 1; there is no need for a forest trust between the CPHCS forest and the DTS forest in Scenario 2.

California Department of Corrections and Rehabilitation / California Prisons Health Care Services: Architectural Considerations
Directory Services Roadmap

Version: 1.04

Date: 14 August 2009

5.1 Scenario 1

This scenario represents a variation of the end-user migration design that had been originally requested by CPHCS. It would only consider the logical migration of CPHCS users and computers; Exchange resources would remain in the CDCR forest. Upon completion of the logical domain migration for CPHCS assets and objects, the migration of Exchange resources for CDCR and CPHCS to DTS would commence. The flow chart for this process is illustrated in Figure 4, below.
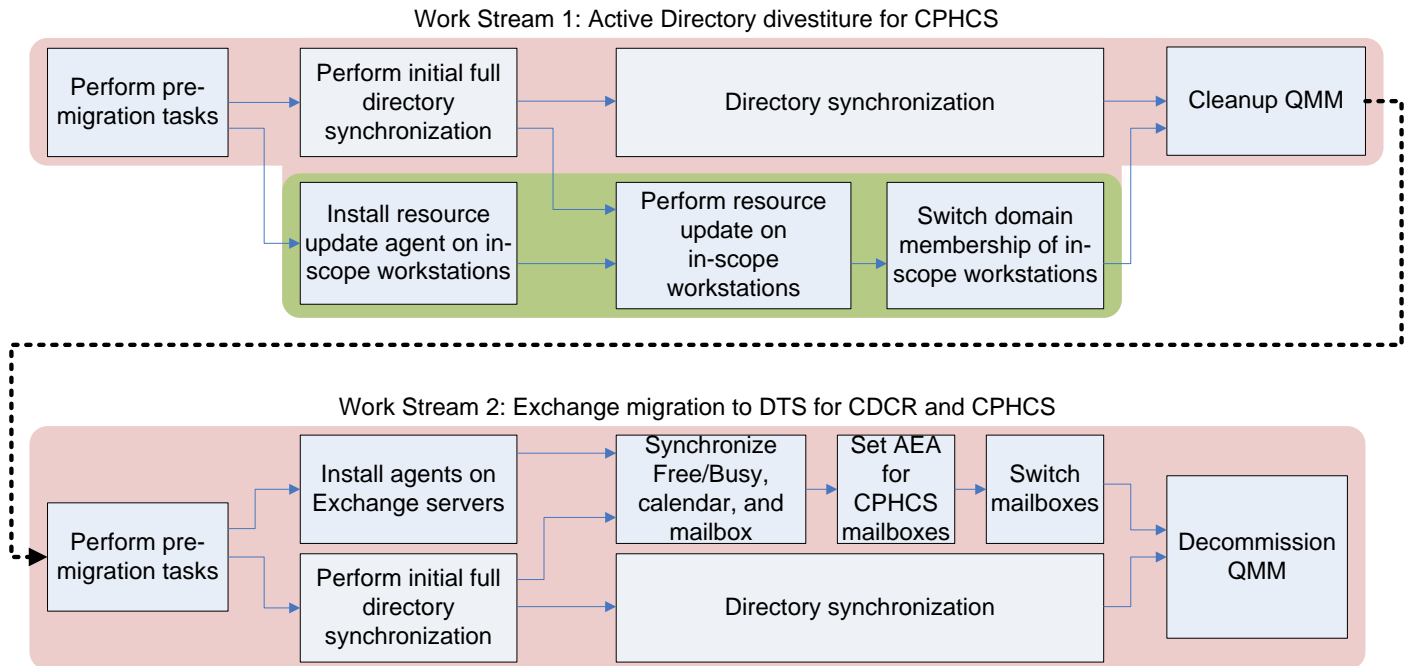
Work Stream 1: Active Directory divestiture for CPHCS

Work Stream 2: Exchange migration to DTS for CDCR and CPHCS

Figure 4 Process flow for Scenario 1

Note: Work Stream 1 and Work Stream 2 can run concurrently, but will introduce risks that could impact users.

Table 1, below, provides a breakdown of pros and cons for this scenario.

Pros	• No architecture changes around directory services • Full ownership and separation. CPHCS can make its decisions without CDCR involvement. • Verizon support model doesn't have to be revisited. • User accounts within the same forest as mission critical apps don't require on trust
Cons	• Data center vendor requirements pose potential additional costs versus keeping users and computers in the CDCR directory. • Migration effort and costs would be repeated if CPHCS users and computers are eventually reintegrated to the CDCR directory. • There is a higher probability of impacting user performance with a migration to a new forest. • The design of email migration to DTS is more complicated and risky considering users would be accessing Exchange from two forests instead of one. • Increased hardware, licensing, and Verizon professional services to accommodate requisite directory services infrastructure to support users and computers at all remote sites. • Allows for the implementation of dissimilar technologies that would need to be overcome if/when CDCR and CPHCS reintegrate. • Complete inventory of CPHCS assets and object is a dependency that must be completed prior to directory migration, which would subsequently delay the Exchange migration to DTS.

Table 1 Pros and Cons for Scenario 1

5.2 Scenario 2

This scenario represents a departure from the requirement to transition CPHCS users and computers to the CPHCS

forest as a first step, although health care applications (e.g. D&T and CDR) would still be staged and managed in the new CPHCS forest at the Torrance data center. Both CDCR and CPHCS users and computers would remain in the existing CDCR forest; gaps for achieving HIPAA compliance in the CDCR directory would be remediated. The migration of Exchange resources to DTS could be started at any point. Additionally, this scenario would not preclude the option of migrating CPHCS users and computers to the CPHCS forest later.

In regard to Verizon IT's involvement, the support services and business requirements would be largely the same:
- Verizon IT will be the first point of contact for CPHCS users and computers.
- Verizon IT will provide support for healthcare applications (D&T, CDR, etc).
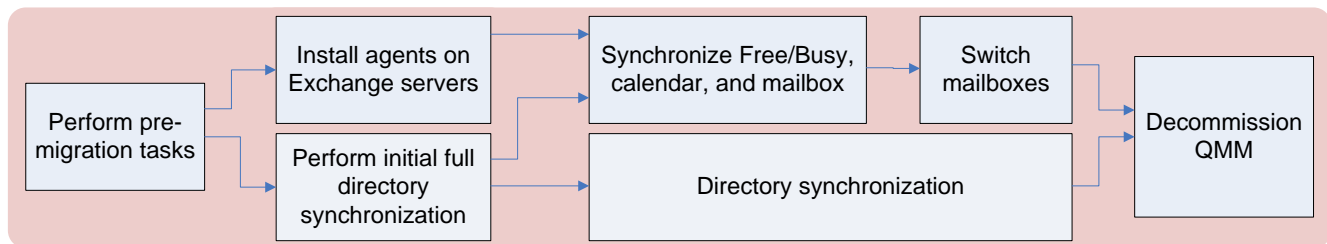- Verizon IT will have full access to health care OUs in CDCR.

Figure 5 Process flow for Scenario 2

Table 2, below, provides a breakdown of pros and cons for this scenario.

Pros	- Leverages the combined numbers of CDCR and CPHCS departments for better bargaining power in all OCIO statewide initiatives. Also makes migration of any services into a statewide system easier. - Implementation of all technology is compatible to both organizations. A steering committee will be required to facilitate this long term partnership. - Straightforward migration to DTS for email. - While implemented as a standalone solution, it does not prohibit implementing Scenario 1 at a later time. - While an inventory of assets and objects will need to be completed in either scenario, it is not a dependency for this scenario. - Less risk for implementations of CDR and D&T applications. - Still supports separation of appropriate resources for HIPAA compliance. - In this scenario, the DTS email migration is not dependent upon the completion of the CPHCS directory migration. - Doesn't hinder any CPHCS timelines for application deployment or addition of new workstations or users. - Doesn't prevent the use of role-based access control.
Cons	- CPHCS would need to coordinate decisions with CDCR. - Verizon support model would need to be revisited. - With a separate directory, licensing costs for applications and services used in the directory might be reduced given that CPHCS and CDCR would only have to purchase licenses for their respective needs.

Table 2 Pros and Cons for Scenario 2

California Department of Corrections and Rehabilitation / California Prisons Health Care Services:
Architectural Considerations
Directory Services Roadmap

Version: 1.04

Date: 14 August 2009

6.   Summary

The assessment of the considered scenarios was based on the input from the attendees and may not reflect non-technical concerns (e.g. political or judicial mandates, etc). In summary, from the perspectives of attendees:

1. Scenario 1 would be more complex and would pose more risk than Scenario 2.
2. Scenario 1 would require email migration to be delayed until the entire CPHCS domain migration is completed.
3. Implementing Scenario 2 now does not prohibit CPHCS from transitioning to Scenario 1 at a later date, if required.
4. Based on all of the information reviewed and presented in this document the technical team unanimously agreed that Scenario 2 is the better solution.

	Scenario 1	Scenario 2
Pros	• No architecture changes around directory services • Full ownership and separation. CPHCS can make its decisions without CDCR involvement. • Verizon support model doesn't have to be revisited. • User accounts within the same forest as mission critical apps don't require on trust	• Leverages the combined numbers of CDCR and CPHCS departments for better bargaining power in all OCIO statewide initiatives. Also makes migration of any services into a statewide system easier. • Implementation of all technology is compatible to both organizations. A steering committee will be required to facilitate this long term partnership. • Straightforward migration to DTS for email. • While implemented as a standalone solution, it does not prohibit implementing Scenario 1 at a later time. • While an inventory of assets and objects will need to be completed in either scenario, it is not a dependency for this scenario. • Less risk for implementations of CDR and D&T applications. • Still supports separation of appropriate resources for HIPAA compliance. • In this scenario, the DTS email migration is not dependent upon the completion of the CPHCS directory migration. • Doesn't hinder any CPHCS timelines for application deployment or addition of new workstations or users. • Doesn't prevent the use of role-based access control.
Cons	• Data center vendor requirements pose potential additional costs versus keeping users and computers in the CDCR directory. • Migration effort and costs would be repeated if CPHCS users and computers are eventually reintegrated to the CDCR directory. • There is a higher probability of impacting user performance with a migration to a new forest. • The design of email migration to DTS is more complicated and risky considering users would be accessing Exchange from two forests instead of one. • Increased hardware, licensing, and Verizon professional services to accommodate requisite directory services infrastructure to support users and computers at all remote sites. • Allows for the implementation of dissimilar technologies that would need to be overcome if/when CDCR and CPHCS reintegrate. • Complete inventory of CPHCS assets and object is a dependency that must be completed prior to directory	• CPHCS would need to coordinate decisions with CDCR. • Verizon support model would need to be revisited. • With a separate directory, licensing costs for applications and services used in the directory might be reduced given that CPHCS and CDCR would only have to purchase licenses for their respective needs.

California Department of Corrections and Rehabilitation / California Prisons Health Care Services: Architectural Considerations
Directory Services Roadmap

Version: 1.04

Date: 14 August 2009

migration, which would subsequently delay the Exchange migration to DTS.	

California Department of Corrections and Rehabilitation / California Prisons Health Care Services:
Architectural Considerations
Directory Services Roadmap

Version: 1.04

Date: 14 August 2009

7.   Attendees and reviewers

The following table provides a list of attendees and reviewers.

Attendee/Reviewer	Organization	Document approval
Zozimo Castro	CPHCS	Approved (via email)
Sean Stokes	CPHCS	Approved (via email)
Scott MacDonald	EIS	Vacation
Peter McCarthy	EIS	Approved (via email)
Kit Chung	EIS	Approved (via email)
Jeff Baker	Microsoft	Approved (via email)
Johnny Martinez	Microsoft	No feedback received
Larry Angus	Angus-Hamer	Approved (via email)
Greg Brown	ENS	Approved (via email)
Brad Lister	CPHCS CDR application	No feedback received
Fred Wood	VIP	Approved (via email)
Uday Kumar	EMC	Approved (via email)
Rob Ross	EMC	Approved (via email)
Eli Hill	Janalent	Approved (via email)